

A SURVEY PAPER ON CLOUD COMPUTING SECURITY AND OUTSOURCING DATA MINING IN CLOUD PLATFORM

A. Hema ¹, S. Visalatchy ¹, C. Mallika ² and N. Ilakkiya ¹

¹ Assistant Professor, Department of MCA, E.G.S. Pillay Engineering College, Nagapattinam.

² Associate Professor, Department of MCA, E.G.S. Pillay Engineering College, Nagapattinam.

ARTICLE INFO

Article History:

Received: 29 Nov 2017;

Received in revised form:

05 Dec 2017;

Accepted: 05 Dec 2017;

Published online: 10 Dec 2017.

Key words:

Security,

Outsourcing,

Cloud Computing,

Data Integrity.

ABSTRACT

In this paper, we tend to discuss regarding a lot of security draw back in cloud computing. In cloud computing techniques rather than data mining square measure accustomed needs great amount information to mine in numerous space of network technology likewise as data mining. As data mining needs great amount of information to be mined rather than investment for resources at constant place, cloud computing resources at constant place.

Copyright © 2017 IJASRD. This is an open access article distributed under the Creative Common Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Cloud Computing overcomes from virtualization, Distribution computing, Grid computing, utility computing and also work on networking, web and software service. Virtualization is helps to run the multiple operating systems with single hardware.

Cloud computing contains three segments such as:

- Applications
- Infrastructure
- Platform

In this paper, we tend to discuss concerning privacy protective problem issues, information integration problems. In cloud Computing and a lot of some improvement in new formula to introduced.

PRIVACY PRESERVING IN CLOUD

In cloud computing, data are stored in multi-locations to make the devices unbiased and also arise the privacy problem. Some research contribution are,

- 1) Security and Privacy in Cloud
- 2) Data Control Using Discretion Algorithm

Cite this article as: Hema, A., Visalatchy, S., Mallika, C., & Ilakkiya, N., "A Survey Paper on Cloud Computing Security and Outsourcing Data Mining in Cloud Platform". *International Journal of Advanced Scientific Research & Development (IJASRD)*, 04 (11/II), 2017, 75 – 78. <https://doi.org/10.26836/ijasrd/2017/v4/i11/41115>.

- 3) Trust and Reputation Management
- 4) TCP and TPM

2.1 Security and Privacy in Cloud

Due to cloud computing, security has lack in many places such as, Google docs, salesforce.com, epic.com, etc... the cloud satisfy with 5 goals as below

- (a) Availability,
- (b) Confidentiality,
- (c) Data integrity,
- (d) Control
- (e) Audit

Cloud provider offer services that may be sorted into 3 categories:

- 1) Infrastructure as a Service (IAAS)
- 2) Platform as a Service (PAAS)
- 3) Software as a Service (SAAS)

2.1.1 Infrastructure as a Service (IAAS)

IAAS provides basic storage and Computing capabilities as Standardised services over the network. Servers, storage system, networking equipment, data centre space etc., are pooled and made available to handle workloads.

2.1.2 Platform as a Service (PAAS)

Platform as a Service is where operating system (such as Window, Android, BSD, iOS, Linux, Mac OS X and IBM z/OS) is hosted “in the cloud”, rather than being physically installed on hardware.

The PAAS layer offers normal remote service with that developers will build application on prime of the computer infrastructure .

2.1.3 Software as a Service (SAAS)

Software as a Service (SAAS) is where most business start their journey to cloud computing; typically starting with the remote delivery of mail and online backup of business information.

Today SaaS is offered by companies such as Google, SalesForce, Microsoft, Zoho, etc. A single instance of the service runs on the cloud and multiple end user are serviced.

2.2 Data Control Using Discretion Algorithm

Using cloud computing system instead of hardware components. It reduces energy cost for running hardware, as well as reducing carbon dioxide emissions. The three main problems in data control such as, First is that the expose of sensitive personal data once exchanging knowledge through the cloud services.

Second one is that the expose people getting Illegal access to information in lack of access control. Third one is that the cloud computing is dynamic surroundings there in service interactions will be created in a more dynamic.

2.3 Trustand Reputation Management

This mechanism used to protect data-centre access and secure data access in cloud computing. In the future, the researchers expect that security as a service (SECaaS) and data protection as a service (DPaaS) will grow rapidly.

2.4. TCP and TPM

Trusted Computing Platform (TCP), which is based on Trusted Platform Module (TPM), into the cloud computing system. TCP used to improve the security, authenticate, integrity and level in cloud computing.

DATA INTEGRITY ISSUES

3.1 Data Integrity Proofs in Cloud Storage

The Service level agreement (SLA), which is given the proof of data integrity, can be agreed by the cloud and customer of cloud. If the customer to check the correctness of his data in the cloud. The disadvantages of data integrity proof in cloud storage as follows .It applies only static storage.

3.2 Data Integration at Scale

The paper describes the evolution of data integrity requirements and given integration solution from the Relational Data Universe starting with the relational data model.

3.3 Data Integrity Check without Original Data

This Scheme based on RSA security algorithm. The advantage of this theme is that the customer does not keep the copy the information with in the cloud. Therefore the theme helps to decrease the storage Space in the cloud.

SECURITY MODEL

4.1 Survey on the Security Model of Cloud

Cloud computing design refers to the parts and subparts needed for cloud computing. These components generally consists of:

- 1) Front End
- 2) Back End

4.1.1 Front End Platform

Cloud computing design consists of front end platform called clients or cloud clients. These clients comprise servers, fat clients, thin clients, zero clients, tablet and mobile devices.

4.1.2 Back End Platform

The back end refers to the cloud itself. It consists of all the resource uired to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanisms, services, deployment models, servers, etc.

OUTSOURCING DATA MINING

5.1 Privacy – Preserving of Outsourcing Mechanisms

To mining the necessary information, from huge amount of data using some mining techniques. In corporate company, some resources are required to mining the data as follows:

- (1) Software tools,
- (2) Hardware infrastructures and
- (3) Human resources.

When an organization hands over its source database to an external party, i.e. called outsourcing. This technique describe the solution should possess the following properties.

- (1) Time efficient,
- (2) Storage efficient,
- (3) High mining precisions.

Its source database to an external party, its data privacy is under the custody of the external party which may not be fully trustworthy.

CONCLUSION

This paper which gives a current trend, security models and data integrity issues in cloud computing. The work related with privacy preserving and outsourcing data mining in cloud computing.

REFERENCES

- [1] Brodie, M. L., (2010) “*Data Integration at Scale: From Relational Data Integration to Information Ecosystems*”, 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010. DOI: [10.1109/AINA.2010.184](https://doi.org/10.1109/AINA.2010.184).
- [2] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A., (2010) “*Security and Privacy in Cloud Computing: A Survey*”, Sixth International Conference on Semantics Knowledge and Grid (SKG), 2010. DOI: [10.1109/SKG.2010.19](https://doi.org/10.1109/SKG.2010.19).
- [3] Jayalatchumy, D., Ramkumar, P., & Kadhivelu, D., (2010) “*Preserving Privacy through Data Control in a Cloud Computing Architecture Using Discretion Algorithm*”, 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010. DOI: [10.1109/ICETET.2010.103](https://doi.org/10.1109/ICETET.2010.103).
- [4] Shen, Z., & Tong, Q., (2010) “*The Security of Cloud Computing System Enabled by Trusted Computing Technology*”, 2nd International Conference on Signal Processing Systems (ICSPS), 2010. DOI: [10.1109/ICSPS.2010.5555234](https://doi.org/10.1109/ICSPS.2010.5555234).
- [5] Kumar, S. R., & Saxena, A., (2011) “*Data Integrity Proofs in Cloud Storage*”, Third International Conference on Communication Systems and Networks (COMSNETS), 2011. DOI: [10.1109/COMSNETS.2011.5716422](https://doi.org/10.1109/COMSNETS.2011.5716422).
- [6] Jing, Z., & Jian-jun, Z., (2010) “*A Brief Survey on the Security Model of Cloud Computing*”, Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010. DOI: [10.1109/DCABES.2010.103](https://doi.org/10.1109/DCABES.2010.103).